REMARKS

Claims 1, 4, and 7-24 are currently pending in the subject application and are presently under consideration. Claims 1, 4, 10 and 14 have been amended as shown on pp. 2-6 of the current reply.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 10 and 14 Under 35 U.S.C §112

Claims 10 and 14 stand rejected under 35 U.S.C §112, first paragraph, as failing to comply with the enablement requirement. Applicants' representative has amended the claims to remove the objectionable material. Applicants' representative respectfully requests that the Examiner withdraw the rejection of claims 10 and 14 under 35 U.S.C. § 112 and pass the application to issue at an early date.

II. Rejection of Claims 1, 4, and 7-24 Under 35 U.S.C. §103(a)

Claims 1, 4, and 7-24 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Lucas et al. (US 6,968,261) in view of Thacker (US Pub. No. 2002/0035696).

As previously stated, applicants' disclosed subject matter relates to detecting malware. The malware evaluator intercepts incoming code/data and searches for malicious code. This can be done by searching the arriving code/data for recognized patterns representative of known malicious code/data. Whereas hackers and the like have come to understand that these searches look for known patterns, the hackers have developed methods of packing malicious executable code to disguise it from traditional virus detecting software. By detecting and unpacking entire packed code packages as they arrive, *e.g.*, intercepting it, the Applicants' invention can maintain the advantage over hackers' attempts at propagating malware through packed malicious executables.

Also as previously presented, the invention of Lucas generally relates to searching code for viruses in an "on-access antivirus system" (*see* Lucas, col. 3, line 47). Lucas describes that hackers have determined a particular weakness in anti-virus software that can cause the anti-virus software to "timeout" when system resources become severely taxed (*see* Lucas, col.1, ln. 11-36). Lucas proposes a solution of decompressing compressed files from a hard drive device

(Lucas, col. 3, ln. 51-52) on-access and scanning these decompressed files for viruses. In Lucas's proposal, malicious files that have been compressed, so as to bog down a system on decompression, can be parsed into smaller decompressed pieces to allow for sequential scanning of each decompressed piece for virus signatures by comparison to DATs (Lucas, col. 4, ln. 7-17). It is to be noted that decompressing and unpacking an entire file is inherently different than decompressing or unpacking only portions of an entire file (*e.g.*, piecemeal or on-access scanning).

As previously stated, Applicants' invention contemplates unpacking entire packed executables, without executing the unpacking code included in a potentially malicious packed executable, to create *corresponding* unpacked executables for analysis. This claimed feature should not be overlooked. The analysis for malware in the subject application is not conducted on an actual unpacked potentially malicious piece of code or data, but rather is conducted on a representation of what the unpacked code/data would look like, but the representation is actually unpacked by a controlled unpacker (*e.g.*, by selectable unpacker modules within the unpacking module) designed to unpack specific file types. This serves to prevent execution of and infection by unpacking of the actual potentially malicious packed executable. This is explicitly claimed in Claim 1, "...receives a packed executable from the malware evaluator and returns an unpacked executable **corresponding** to the **entire** packed executable...", (emphasis added). Lucas neither explicitly nor implicitly discloses this feature of the claimed invention. Thacker does not cure this deficiency.

The Examiner has rejected Claim 4 based on similar reasoning as applied to Claim 1, Applicants' representative therefore similarly disagrees with the Examiner's position. In particular, independent claim 1 recites, "....the unpacked executable **corresponding** to the **entire** packed executable" (emphasis added). Contrary to assertions made in the Office Action, the cited reference, for the reasons disclosed herein above with respect to Claim 1, does not disclose or suggest this feature of Applicants' claimed invention. Thacker does not cure this deficiency.

Therefore, based on the above remarks, the Applicants respectfully request that the Examiner withdraw the rejection of Claims 1 and 4 under 35 USC § 103(a) as being anticipated by Lucas in view of Thacker.

Claims 7-24 each rely on aspects of unpacking *entire* packed executables and thus the cited art suffers the same problems as described above. Applicants' representative therefore

further asserts that these claims are patentably distinct over Lucas either alone or in combination with Thacker. For example, Claims 7 and 8 recite features of unpackers employed in returning a corresponding executable; Claims 13 and 15-17 recite features of determining malware with regard to code/data that is not a packed executable; and Claims 19-24 recite features of methods including corresponding executable aspects, aspects of intercepting code/data from networks and distributable media, and aspects of unpacking entire executables, among others.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP2193US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Frank J. Schumacher IV/
Frank J Schumacher IV
Reg. No. 61,292

AMIN, TUROCY & CALVIN, LLP
57TH Floor, Key Tower
127 Public Square
Cleveland, Ohio 44114
Telephone (425) 256-8302
Facsimile (216) 696-8731